

INTEGRATED DATA TRAFFIC MONITORING SYSTEM**Abstract of the Disclosure**

5 The present invention includes an integrated data traffic monitoring system monitoring data traffic on a computer system. The monitoring system includes a security appliance and one or more security and monitoring technologies such as hardware and open source and proprietary software products. The security appliance and the security and monitoring technologies may be implemented as separate and distinct modules or combined into a single security appliance. The security and monitoring technologies monitor network data traffic on, or directed to, the computer system. The monitoring system collects data from each of the technologies into an event database. The contents of the event database are continuously analyzed for possible threats to the computer system. In some cases, the analysis may determine that messages with certain attributes are potential threats and feedback, in the form of alerts, notifications, commands, or instructions, may be provided to one or more of the technologies.

10